IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

NO. 5:13-CR-328-FL

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | ) | |
| | ) | |
| v. | ) | |
| | ) | ORDER |
| NIKHIL NILESH SHAH, | ) | |
| | ) | |
| Defendant. | ) | |

This matter comes before the court on three motions of defendant Nikhil Nilesh Shah to suppress evidence obtained in violation of defendant's Fourth and Fifth Amendment rights (DE 23, 24, 25). The government timely filed a response in opposition to defendant's motions, to which defendant replied. The issues raised are ripe for ruling. For the reasons that follow, the court denies defendant's motions.

**STATEMENT OF THE CASE**

On December 17, 2013, a grand jury returned a one-count indictment charging defendant with intentional damage to a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B)(i), and 1030(c)(4)(A)(i)(I). After a period of discovery, defendant filed the instant motions to suppress on June 30, 2014.

Defendant asserts that the government violated his Fourth Amendment rights when it acquired "cell phone location evidence" for AT&T Wireless telephone numbers associated with defendant, along with "user location information" obtained from Facebook, Inc. ("Facebook"). (Mot. To Suppress Tracking Data, 13) (DE 25). Defendant also asserts Fourth Amendment violations based upon government seizure of email communications and associated data from

Google, Inc. ("Google"). (DE 24). Finally, defendant asserts that government agents violated his Fifth Amendment rights by confronting him with evidence after he had requested an attorney. (DE 23).

The government filed a combined response in opposition to defendant's three suppression motions on August 30, 2014. The government argues that defendant has no reasonable expectation of privacy in the information obtained from AT&T Wireless and Facebook because the records are business records created and held by the respective service providers. As to defendant's motion regarding emails and associated information obtained from Google, the government argues that the search warrant for this information ("Google Warrant") complied with the Fourth Amendment because it was supported by probable cause, and particularly described the information to be searched and the procedure for seizure. Alternatively, if the court finds that the challenged evidence was obtained in violation of defendant's Fourth Amendment rights, suppression should not be ordered, it argues, because the government reasonably relied in good faith on the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, *et seq.*, and upon orders from a magistrate judge issued pursuant to § 2703(d).[1] Finally, the government responds to defendant's motion seeking suppression of evidence generated during his arrest that it will not attempt to offer into evidence any of the statements or conduct discussed in defendant's motion to suppress on Fifth Amendment

[1] Section 2703(d) provides, in relevant part:

> A court order for disclosure [for contents or records of wire or electronic communications] may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation . . . .

18 U.S.C. § 2703.

grounds, rendering that motion moot. Defendant's reply, filed September 4, 2014, after seeking leave, concentrates on the government's stated opposition to his motion to suppress tracking data obtained without a warrant.

The complexity of issues presented has necessitated a more extended period of time for the court's decision making. Arraignment and trial was continued in this case until no sooner than 45 days after disposition of the instant motions. In accordance with the court's order entered July 30, 2014, the clerk now will set the matter for arraignment and trial at the court's next regular criminal term no sooner than 45 days from date of entry of this order.

## FACTUAL BACKGROUND

Defendant was formerly an Information Technology Manager at Smart Online, Inc. ("SOLN"), a mobile application development company in Durham, North Carolina. On June 28, 2012, after defendant was no longer a SOLN employee, an intruder accessed the SOLN computer network and caused significant damage. On June 29, 2012, SOLN and the Durham Police Department initiated an investigation, which was later joined by the FBI. As part of the investigation, the FBI filed an application for a search warrant targeting the electronic mail address shahnn28@gmail.com. The Google Warrant issued from a magistrate judge on November 5, 2012.

The Google Warrant references Attachment A as the "the property to be searched." (Google Warrant, at 2) (DE 24-1.) Attachment A provides that the warrant applies to "information associated with SHAHNN28@GMAIL.COM that is stored on premises controlled by Google, Inc." (Id. at 4). For the "property to be seized," the affidavit references Attachment B. Section I of Attachment B details particular items of "Information to be disclosed by Google," including:

> a. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination

addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, Google search history, and files;

d. All records pertaining to communications between including [sic] contacts with support services and records of actions taken.

(Google Warrant, 5-6). Section II of Attachment B specified that the information "to be seized by the government" would include

> [a]ll information described above in Section I that constitutes fruits, evidence, and instrumentalities of Title 18, United States Code, Sections 1030 (Fraud and Related Activity in Connection with Computers), since account inception, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:
>
> a. Preparatory steps taken in furtherance of unauthorized network activity, communications regarding execution of the unauthorized network activity, and information regarding tools used in furtherance of the unauthorized network activity.
>
> b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

(Id. at 6).

As alleged by defendant, agents used the Google Warrant to obtain "over 1GB [gigabyte] of data associated with the shahnn28@gmail.com [account], including emails, chats, and other information spanning from roughly March 6, 2007 through November of 2012." (Mot. To Suppress

Email and Related Evidence, 3) (DE 24). According to the government, the data "revealed that on June 29, 2012 at 4:46 PM, [defendant] sent himself an e-mail ("June 29 Email") to shahnn28@gmail.com from shahnn28@gmail.com with no subject line that contained three website links related to Cisco ASA VPN and PIX firewall configurations." (Gov. Resp., 8) (DE 35). These firewall configurations were used by SOLN in its network infrastructure. The links in the June 29 Email directed to web pages that discuss security settings for these devices. Furthermore, the Internet Protocol (IP) address associated with the June 29 Email was also identified as connecting to the SOLN network. The IP address had also been used previously to send emails to SOLN employees. The government determined that the IP address was geographically located in Holly Springs, North Carolina, the city of defendant's residence at the time of the intrusion.[2]

The government also alleges that, although defendant contacted SOLN employees on June 28 and June 29, 2012, to report receiving security alerts regarding the SOLN network, a review of the email account shows that he never received any such alerts. Furthermore, chat sessions stored in the email account revealed that defendant had boasted of having access to the SOLN network and of performing the June 28, 2012 intrusion.

Subsequent to obtaining the Google Warrant, the government submitted two applications pursuant to Section 2703(d) of the SCA. On February 25, 2013, the magistrate judge issued an order requiring AT&T Wireless to disclose "[a]ll records and other information (not including the contents of communications) relating to the [referenced] [a]ccount," including "[r]ecords of user activity for each connection made to or from the account[;] . . . [i]nformation about each communication sent or received by the [a]ccount, including the date and time of the communication, the method of

[2] It is not clear whether the geographical location of this IP address was also obtained via the Google Warrant.

communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers)" and "[a]ll data about which 'cell towers' i.e. antenna towers covering specific geographic areas) and 'sectors' (i.e., faces of the towers, received a radio signal from each cellular telephone or device assigned to the Account." (AT&T Wireless Order, at 5) (DE 26-1). The AT&T Wireless Order specified that the time period for this information would span from June 1, 2012 through February 12, 2013.

Agents obtained from AT&T Wireless records that were created and maintained when the cell phone associated with the accounts transmitted a signal to a cell tower to connect communications. Defendant alleges that "[t]he information produced by AT&T allowed the government to pinpoint the geographic location of [defendant's] cell phone for over half a year." (Mot. To Suppress Tracking Data, 2). The government's response suggests the information revealed that defendant exchanged text messages with a SOLN employee around the time of the network intrusion. A cell phone tower located close to defendant's Holly Springs residence facilitated these communications.

Nearly a month later, on March 19, 2013, pursuant to another Section 2703(d) request from the government, the magistrate judge issued an order for records from Facebook, Inc. ("Facebook Order") (DE 26-2). The order directed Facebook to provide "[a]ll records and other information (not including the contents of communications relating to the [referenced] Account." (Id. at 4-5). It specifically provided for disclosure of information concerning the account holder's IP addresses, times of connections made to Facebook, times of communications sent or received by the account, and the source and destination of IP addresses. (Id. at 5). As in the AT&T Wireless Order, the information spanned from June 1, 2012 to February 12, 2013. Information provided by Facebook

pursuant to the order includes the account holder's IP addresses, the time of the account holder's Facebook activity, a general description of the type of Facebook interaction or activity performed (e.g. "Login" or "Session updated"), and the account holder's city, region, and country at the time of the activity.[3] The government provides sample pages of Facebook's response at Exh. 3. (Gov. Resp., Exh. 3) (DE 35-3).

In both the AT&T Order and the Facebook Order, the magistrate judge found that the government had "offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing investigation." (AT&T Wireless Order at 2; Facebook Order at 2).

Defendant was arrested in New Jersey on January 8, 2014, by agents from the FBI. According to an investigative report dated January 15, 2014, defendant "immediately requested his attorney be present during any subsequent questioning." (Investigative Report Pertaining to the Arrest and Interview of Nikhil N. Shah, at 2) (DE 23-1). Agents transported defendant from his residence to the Newark, New Jersey FBI building, where he was placed in an interview room. Agents proceeded to review the evidence against defendant. In response, defendant provided agents with allegedly incriminating conduct and statements.

## DISCUSSION

A. Motion to Suppress Location Data Obtained Without a Warrant (DE 25)

Defendant argues that the government's warrantless acquisition of records from AT&T and Facebook violated his Fourth Amendment rights. Although defendant seeks suppression of "all information obtained by the government pursuant to 18 U.S.C. § 2703(d) without the issuance of

[3] The parties dispute the accuracy of the location information provided by Facebook. The court does not find it necessary to resolve this dispute to rule on the issues raised.

a warrant supported by probable cause," (Mot. To Suppress Tracking Data, 1) his arguments focus on data that revealed his geographic location at particular times. (See Id., 13) (concluding that, "because the cell phone *location* evidence from AT&T and the user *location* information from Facebook was obtained in violation of [defendant's] Fourth Amendment rights, suppression of all *location* tracking evidence obtained by the government pursuant to 18 U.S.C. § 2703(d) should be ordered.") (emphasis added).

The records at issue were obtained pursuant to the SCA, 18 U.S.C. §§ 2703(c)(1) and (d). Section 2703(c)(1) states that the government "may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service" under specified circumstances. 18 U.S.C. § 2703(c)(1). These circumstances include when the government obtains a warrant, when the subscriber or customer has given his or her consent, or, as is the case for the location data obtained here, when the government "obtains a court order for such disclosure under subsection (d) of this section," (i.e. section 2703(d)). 18 U.S.C. § 2703(c)(1)(A)-(E). The records that the government may obtain pursuant to section 2703(c)(1) exclude "the contents of communications." 18 U.S.C. § 2703(c)(1).

Under section 2703(d), an order for disclosure "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[ ] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). While defendant does not expressly attack the statute's constitutionality, he argues that the AT&T Order and Facebook Order were unconstitutional.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and

no warrants shall issue, but upon probable cause, and particularly describing the place to be searched, and the persons or things to be seized." Ordinarily, a "search . . . is 'unreasonable' unless it has been authorized by a valid search warrant, and in cases in which the Fourth Amendment requires that a warrant to search be obtained, 'probable cause' is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness." United States v. DeQuasie, 373 F.3d 509, 518 (4th Cir. 2004) (quoting Camara v. Municipal Court of San Francisco, 387 U.S. 523, 528-29 (1967)). Defendant bears the burden of establishing a violation of his Fourth Amendment rights. Rakas v. Illinois, 439 U.S. 128, 130, n. 1 (1978).

Legislative history behind section 2703(d) states that the standard used for such orders is "higher than a subpoena, but not a probable cause warrant." Senate Report No. 103-402 , at 31 (1994); H.R. Rep. No. 103-827, pt. 1 at 31 (1994). Based upon this legislative history, courts have determined that the standard applicable to court orders under section 2703(d) of the SCA is easier for the government to satisfy than probable cause. In re App. of the U.S. Directing a Provider of Elec. Communication Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313-15 (3rd Cir. 2010) (holding that, in light of legislative history, the section 2703(d) standard was "a lesser one than probable cause."); see also United States v. Graham, 846 F. Supp. 2d 384, 396 (D. Md. 2012).

The Supreme Court has observed that its "Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th Century." United States v. Jones, 132 S. Ct. 945, 949 (2012). However, in more recent cases the Court has extended the protection to situations where "government officers violate a person's 'reasonable expectation of privacy.'" Id. at 950 (citing Katz v. United States, 389 U.S. 347, 360 (1967)). A two-fold requirement applies to whether an individual has a reasonable expectation of privacy: first, the individual must have

demonstrated "actual (subjective) expectation of privacy," and second, "the expectation [must] be one that society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361; see also United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010).

An individual does not have a "reasonable expectation of privacy" in information that is "revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976). In Smith v. Maryland, the court considered whether the installation and use of a monitoring device known as a pen register constitutes a "search" within the meaning of the Fourth Amendment. Smith v. Maryland, 442 U.S. 735, 736 (1979). The pen register was installed at the telephone company's offices, and recorded the numbers dialed on Smith's telephone through the electrical impulses produced by release of the telephone dial. Id. at 736 n. 1, 737. The Court held that Smith had no "legitimate expectation of privacy" regarding the numbers he dialed on his phone. Smith, 442 U.S. at 742. Applying Katz and Miller, the Court reasoned that, "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial." Id. Moreover, the Court held that "even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable" because, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at 743-44 (quotation marks and citations omitted).

In Bynum, the FBI subpoenaed Yahoo!, Inc. ("Yahoo") for subscriber information entered into the Yahoo website when Bynum opened his account, along with IP addresses associated with uploads of child pornography to that website. Bynum, 604 F.3d at 162. Once the FBI obtained this

information, it subpoenaed the internet service provider associated with the IP addresses and obtained Bynum's email address and telephone number. Id. at 162-63. The FBI also subpoenaed records from telephone and internet companies that operated Bynum's dial-up internet service. Id. at 163. Using this information, the FBI located Bynum's name and physical address. Id. at 163. The Fourth Circuit held that Bynum failed to point to any evidence that he had a subjective expectation of privacy in the subscriber information, as he had "voluntarily conveyed all this information to his internet and phone companies." Id. at 164.[4] Moreover, even if Bynum had such a subjective expectation, the court held it would not be objectively reasonable. Id. Consequently, issuance of the subpoenas did not violate the Fourth Amendment.

Defendant's motion challenges two forms of location data: the data that was obtained from AT&T Wireless's records, purportedly showing the location of defendant's cell phone, and data that was obtained from Facebook's records, purportedly showing defendant's location when he accessed Facebook at various times. Applying these principles, the court analyzes the government's acquisition of these two forms of location data separately below.

1. Records Obtained from AT&T Wireless

The basic process by which the cell phone location data was obtained is not in dispute. The government's brief explains that a cell phone user "transmits a signal to a cell tower for his call to be connected, and the provider thereby creates records, for its own business purposes, regarding

[4] The court did not address whether Bynum had likewise voluntarily conveyed the IP addresses obtained from Yahoo, because Bynum had abandoned his argument that he had such a privacy interest in that information. Bynum, 604 F.3d at 164, n.2.

which of its cell towers it used to complete the call." (Gov. Resp., 18).[5] Such data is also known as "cell site location data." E.g. Graham, 846 F. Supp. 2d at 386.

Although the Fourth Circuit has not directly addressed the issue raised here, most courts which have considered a Fourth Amendment challenge to collection of this data under the SCA have relied on the rules regarding third party/business records, as provided under Miller and Smith, to uphold the government's action. See In re U.S. for Historical Cell Site Data, 724 F.3d 600, 612-15 (5th Cir. 2013); United States v. Giddins, — F. Supp. 3d —, 2014 WL 4955472, at *8 (D. Md. 2014); Graham, 846 F. Supp. 2d at 389 (collecting cases). Such courts reason that no expectation of privacy applies because cell phone users voluntarily convey the cell site location data to their providers. In re U.S. for Historical Cell Site Data, 724 F.3d at 611-13; Giddins, — F. Supp. 3d —, 2014 WL 4955472 at *8; Graham, 846 F. Supp. 2d at 389; United States v. Suarez-Blanca, No. 07-023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. April 21, 2008).

In addition, on finding that the SCA conforms with existing Supreme Court precedent interpreting the Fourth Amendment, courts have declined to find that society would recognize that an expectation would be reasonable. See In re U.S. for Historical Cell Site Data, 724 F.3d at 614-15; Giddins, — F. Supp. 3d —, 2014 WL 4955472 at *10; Graham, 846 F. Supp. 2d at 405. As such, these courts have held that the government does not violate the Fourth Amendment in acquiring cell site location data from a service provider. Id.

The court finds the reasoning underlying these cases persuasive in denying defendant's

[5] See also In re Application of United States, 849 F. Supp. 2d 526, 534 (D. Md. 2011) ("Cellular identification locates a user by triangulating their position based on the cell towers within signal range of their mobile phone.") (quoting The Collection and Use of Location Information for Commercial Purposes: Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection and Subcomm. on Communications, Technology, and the Internet of the H. Comm. on Energy and Commerce, 111th Cong. 3 (2010) (statement of Lori Faith Cranor, Professor of Computer Science and of Engineering & Public Policy, Carnegie Mellon University).

motion. The cell site location data obtained here voluntarily was conveyed to AT&T Wireless, and is part of the company's business records. Under Smith and Miller, such voluntarily conveyed information, kept as a business record, is not protected by the Fourth Amendment. Smith, 442 U.S. at 742, 743-44; Miller, 425 U.S. at 443.

Defendant cites to the Supreme Court in arguing that the cell site location data at issue here violates the Fourth Amendment. Defendant points to the case of United States v. Karo to argue that locating an individual's cell phone "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance." United States v. Karo, 468 U.S. 705, 707 (1984). Karo involved the secret installation of a radio beeper in a can of ether, which was then traced to defendant's home. Id. at 708-10. The case did not involve business records, and Karo was not voluntarily conveying his geographic location. Karo simply does not control here.

Defendant next argues that the Supreme Court's decision in Jones requires exclusion of the tracking evidence obtained from AT&T Wireless. The Supreme Court held in that case that the attachment of a Global-Positioning-System (GPS) tracking device on a suspect's vehicle, and subsequent use of that device to monitor the vehicle's movement, constituted a "search." Jones, 132 S. Ct. at 949. However, the majority opinion in Jones relied on the Fourth Amendment's origins in common-law trespass to find that the government had performed a search. Id. ("The government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."). No such physical intrusion is alleged here.

Defendant nevertheless argues that concurring opinions in Jones demonstrate that five of the justices agree that "when the government engages in prolonged location tracking, it conducts a search under the Fourth Amendment." (Mot. To Suppress Tracking Data, 4). One of these concurring opinions, authored by Justice Alito and joined by Justices Ginsburg, Breyer and Kagan, articulated that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Id. at 964. In a separate concurring opinion, Justice Sotomayor (who had also joined the majority opinion), agreed with that statement. Id. at 955-56. Thus, a majority of the justices appeared willing to accept that long-term surveillance conducted via a GPS device can become a search triggering Fourth Amendment concerns.

However, it is not clear how these five justices would rule on the circumstances at issue here, where a GPS device was not used, the tracking information is historical, rather than real-time, and a federal statute expressly provides for the method by which the location information was obtained. Indeed, some parts of Justice Alito's concurrence would support denial of defendant's motion. Justice Alito wrote that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative . . . . A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." Jones, 132 S. Ct. at 964. Drawing on this opinion, some courts have held that, if society is prepared to recognize a greater expectation of privacy, the legislature is the appropriate body to make such a pronouncement. See In re U.S. for Historical Cell Site Data, 724 F.3d at 615 ("[T]he recourse for these desires [to keep cell site location data private] is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections."); Giddins, — F. Supp.

3d —, 2014 WL 4955472 at * 10 ("Congress has determined the appropriate balance to be struck. If the arc of technological improvement (or the implementation of that technology by the government) should be altered in a way that does infringe a person's legitimate expectation of privacy, the solution is properly for the legislature to address.") (quoting Graham, 846 F. Supp. 2d at 390) (quotation marks omitted).

In addition to the Jones concurrences, defendant relies heavily on the Eleventh Circuit's recent opinion in United States v. Davis, which found Jones instructive in holding that the collection of cell site location data violated defendant's reasonable expectation of privacy. United States v. Davis, 754 F.3d 1205, 1214-17 (11th Cir. 2014). However, Davis has been vacated pending hearing *en banc*. United States v. Davis, 573 F. App'x 925 (11th Cir. 2014).

Defendant also argues that the Supreme Court's decision in Riley v. California, issued earlier this year, dictates that the tracking records obtained from AT&T Wireless be suppressed. Riley v. California, 134 S. Ct. 2473 (2014). In Riley, the Court held that police could not search digital information on a cell phone seized from an individual who had been arrested without a warrant. Riley, 134 S. Ct. at 2489, 2495. The Court noted the immense storage capacity of cell phones, and declared that they "hold for many Americans the 'privacies of life.'" Id. at 2495. However, Riley expressly distinguished Smith, because the government did not dispute that a search had occurred. Id. at 2492-93. Other courts have rejected the argument that Riley compels suppression of cell site location data obtained under section 2703(d). See United States v. Guerrero, 768 F.3d 351, 359-60 (5th Cir. 2014); Giddins, — F. Supp. 3d —, 2014 WL 4955472, at * 7.

Defendant's authorities do not persuade the court to depart from the precedents of Miller, Smith, Bynum, or the persuasive reasoning underpinning decisions by a majority of courts that have

considered the government's collection of cell site location data under section 2703(d) of the SCA. The government's actions in obtaining AT&T Wireless records did not violate the Fourth Amendment. Thus, defendant's motion as to these records is denied.

2. Records Obtained from Facebook

Defendant's Fourth Amendment claim also fails as it applies to the records obtained from Facebook. As noted, these records included information regarding the Facebook account holder's IP addresses, the time of the account holder's Facebook activities, a general description of the Facebook activity, and the Facebook account holder's city, region, and country at the time of the activity. (See Gov. Resp., Exh. 3 at 2-5). Defendant relies on the same cases noted above, regarding tracking geographic location, to argue that the government's acquisition of this information violated the Fourth Amendment.

Defendant again fails to show that any Fourth Amendment search occurred. The cases cited above found that the conveyance of cell site location data is a voluntary action, performed for the purpose of obtaining service. See In re U.S. for Historical Cell Site Data, 724 F.3d at 612; Giddins, — F. Supp. 3d —, 2014 WL 4955472 at *9. Similarly, in Bynum the court held that defendant had voluntarily conveyed his name, email address, telephone number and physical address to his telephone and internet companies. Bynum, 604 F.3d at 164.

In a recent case, the Eastern District of Virginia also found that certain internet users who had filed a petition to quash a § 2703(d) order had voluntarily conveyed their IP addresses to the social media service known as Twitter. In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 135-36 (E.D. Va. 2011) ("E.D. Va. § 2703 Order"). The court found that web sites can easily determine the IP address of the computers which seek to access

the site. Id. at 120. It noted that "[m]ost websites maintain standard logs of connecting IP addresses, along with date and time information, and may even include information about the user associated with the connection." Id. It held that IP addresses were similar to phone numbers because both "must be revealed to intermediaries as a practical necessity of completing communications over their respective networks . . . . Both are automatically revealed to the other party and any intermediaries carrying the communication." Id. See also United States v. Christie, 624 F.3d 558, 574 (3rd Cir. 2010) ("[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties . . . ."); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.").

It is not clear exactly how Facebook obtained the information which defendant seeks to suppress here. The lack of evidence also strikes against defendant's motion. As noted, defendant bears the burden of establishing a violation of his Fourth Amendment rights. Rakas, 439 U.S. at 130, n. 1. This includes the burden of showing a subjective expectation of privacy and an expectation that is reasonable. See Bynum, 604 F.3d at 164 ("Bynum can point to no evidence that he had a subjective expectation of privacy in his internet and phone 'subscriber information.' "); United States v. Burgess, 836 F. Supp. 336, 338 (D.S.C. 1993).

On the present record it appears that Facebook obtained some location information about defendant. Defendant has argued only that the location information held by Facebook should not be disclosed because it tracks his movements; he has not alleged that he never disclosed the information to Facebook, nor has he given any reason to believe that such disclosure was

involuntary. Defendant has failed to carry his burden of proof as to holding a reasonable expectation of privacy, and his motion is denied with respect to the Facebook user location information as well.[6]

B. Motion to Suppress Email and Related Evidence (DE 24)

The analysis set out above applies also to some of the information obtained with the Google Warrant. So far as the Google Warrant authorized acquisition of non-content "records" regarding the account, such as the account identification information noted under subsection (b) to Section I of Attachment B, there seems to be no meaningful distinction between this information and the "subscriber information" which Bynum found to be outside the Fourth Amendment's protection. Bynum, 604 F.3d at 164. Similarly, defendant has failed to show any reasonable expectation of privacy in records of communications that he had with Google support services and the subsequent actions taken by Google, as noted under Attachment B, Section I(d). These communications were made to Google, and both communications and subsequent actions became part of Google's business records when stored.

In contrast, some other information obtained through the Google Warrant is indeed protected by the Fourth Amendment. With respect to subsection (a) in Section I of Attachment B to the Google Warrant, authorizing a search through the contents of all emails, courts have recognized that such information is protected by the Fourth Amendment, despite being held on an email account maintained by a third-party. See United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails . . . ."); Forrester, 512 F.3d at 511 ("The contents [of emails] may deserve Fourth Amendment protection."); United States

[6] Because the court finds no Fourth Amendment violation, it need not reach the government's argument that agents acted in "good faith" in relying on the magistrate judge's orders. In any event, analysis of "good faith" is made more difficult here, where supporting documentation to the application for the AT&T Wireless Order and Facebook Order have not been entered into the record. "Good faith" is analyzed with respect to the Google Warrant below.

v. Ali, 870 F. Supp. 2d 10, 39 n. 39 (D.D.C. 2012); United States v. Bode, No. ELH-12-158, 2013 WL 4501303, at *15 (D. Md. Aug. 21, 2013); see also United States v. Hamilton, 701 F.3d 404, 408 (4th Cir. 2012) (recognizing, in marital privilege context, that "one may generally have a reasonable expectation of privacy in email").

Likewise, although the subject does not appear to have previously been addressed by courts in this circuit, other courts have suggested that persons have a privacy interest in information such as that sought under section I(b), including "address books, contact and buddy lists, calendar data, pictures and files." See In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 2013 WL 4647554, at *7 (D. Kan. Aug. 27, 2013); United States v. Bickle, No. 2:10-CR-565, 2011 WL 3798225, at *21-22 (D. Nev. July 21, 2011).

By including requests for "the contents of all e-mails," (Google Warrant, at 5), the Google Warrant implicates a different subsection of the SCA than the location data noted above, which, as noted, applies to records "not including the contents of communications." 18 U.S.C. § 2703(c)(1); see also E.D. Va. § 2703 Order, 830 F. Supp. 2d at 129 (distinguishing between "*content* information about a communication," to which paragraphs (a) and (b) apply, and "non-content *records*," governed by paragraph (c)"). Sections 2703(a) and (b)(1)(A) of the SCA provide for the government to require "disclosure" of "the contents of a wire or electronic communication" from "a provider of electronic communication service" or "a provider of remote computing service" pursuant to a warrant under the Federal Rules of Criminal Procedure. "Contents" are defined as "information concerning the substance, purport, or meaning of that communication." 18 U.S.C. §

2510(8). These sections of the SCA governed the use of the Google Warrant to obtain the contents of emails and other information associated with the account shahnn28@gmail.com.

Defendant essentially challenges the Google Warrant on four grounds, arguing that: 1) the warrant terms "failed to provide a meaningful limit on searcher discretion" (Mot. To Suppress Email and Related Evidence, 5); 2) the provision for items "to be disclosed by Google" in Section I of Attachment B effectively permitted an unconstitutional seizure within the meaning of the Fourth Amendment; 3) the warrant should have provided "a method, such as a filter team, for avoiding or minimizing sweeping unauthorized emails and computer data into the search," (Id., 9); and 4) the government's inspection of email communications exceeded the scope of the warrant. As explained below, the court agrees that the warrant's terms failed to provide the necessary particularity because they failed to state the particular crime for which the evidence was being sought. Nevertheless, the evidence is admissible because officers acted in "good faith" in relying on the Google Warrant. Furthermore, the disclosure provision and methods provided by the Google Warrant complied with the Fourth Amendment. Also for reasons discussed, the court finds the defendant has failed to meet his burden of showing that the government exceeded the scope of the warrants.

1. Limits on Searcher Discretion

As noted above, the Fourth Amendment states that "no warrants shall issue, but upon probable cause." "Although the concept of probable cause resists an exacting definition, it exists where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found in a particular place." United States v. Hurwitz, 459 F.3d 463, 473 (4th Cir. 2006) (quoting United States v. Perez, 393 F.3d 457, 461 (4th Cir.2004)) (quotation marks and brackets omitted). The probable cause determination requires

consideration of "the totality of the circumstances." Maryland v. Pringle, 540 U.S. 366, 371 (2003). A warrant must be "no broader than the probable cause on which it is based." Hurwitz, 459 F.3d at 473.

As a related concept to a warrant tailored to probable cause, the Fourth Amendment requires that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." See also In re Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 856 (9th Cir. 1991) ("Specificity [of a warrant] has two aspects: particularity and breadth . . . . Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based."). The requirement of "particularity" prevents the government from acting under a "general warrant," whereby law enforcement undertakes "a general, exploratory rummaging in a person's belongings." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). "The particularity requirement is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description of the items leaves nothing to the discretion of the officer executing the warrant." United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010). The test for particularity "is a pragmatic one," in which "[t]he degree of specificity required when describing the goods to be seized may necessarily vary according to the circumstances and type of items involved . . . [T]here is a practical margin of flexibility permitted by the constitutional requirement for particularity in the description of the items to be seized." United States v. Torch, 609 F.2d 1088, 1090 (4th Cir. 1979).

In order to satisfy particularity, the warrant must "at least minimally confine[ ] the executing officers' discretion by allowing them to seize only evidence of a *particular crime*." United States v. Dickerson, 166 F.3d 667, 693 (4th Cir. 1999) (emphasis added), rev'd on other grounds, 530 U.S.

428 (2000). Dickerson distinguished between evidence of a "particular crime" and evidence related to "general criminal activity" as follows:

> a warrant authorizing a search for evidence relating to "a broad criminal statute or general criminal activity" such as "wire fraud," "fraud," "conspiracy," or "tax evasion," is overbroad because it "provides no readily ascertainable guidelines for the executing officers as to what items to seize" . . . . In contrast, a warrant authorizing a search for evidence relating to "a specific illegal activity," such as "narcotics," or "theft of fur coats" is sufficiently particular.

Id. at 694 (citing United States v. George, 975 F.2d 72, 76 (2nd Cir. 1992)). In Dickerson, the warrant authorized seizure of "[e]vidence of the crime of bank robbery." Id. at 693. The court held that "bank robbery" was a "specific illegal activity that . . . generates quite distinctive evidence," and thereby upheld the warrant. Id.

The items to be disclosed pursuant to Section I(a) and (c) of Attachment B include broad categories of documents, including "[t]he contents of all e-mails stored in the account. . . .," and "[a]ll records or other information stored by an individual using the account . . . ." (Google Warrant, 5). The government offers no argument that it could seize and retain all of this information, but focuses on the "two step" nature of the warrant, whereby the information provided in Section I was "disclosed," and would only be "seized" if it met the criteria noted in Section II.

However, the terms of Section II are likewise expansive. The provision describing the documents "seized" makes a general reference to "[a]ll information described above in Section I that constitutes fruits, evidence, and instrumentalities of Title 18, United States Code, Sections 1030 (Fraud and Related Activity in Connection with Computers)." (Google Warrant, 6). This statute, also known as the federal Computer Fraud and Abuse Act ("CFAA"), prohibits a wide array of activities, including the use of computers to transmit information restricted by the United States without authorization, intentionally accessing a computer without authorization or exceeding

authorized access to obtain financial records, accessing nonpublic computers of the United States in a way which affects the government's use, accessing protected computers without authorization in order to commit fraud, threatening to cause damage or obtain information from a protected computer, conspiracy to commit these offenses, and other activities. See 18 U.S.C. § 1030(a).

A violation of the CFAA would not necessarily generate such "distinctive evidence" as bank robbery or narcotics. Dickerson, 166 F.3d at 694. Nor would evidence necessarily be as distinctive as that of child pornography, a type of crime more commonly targeted by warrants for electronic information. E.g. United States v. Schesso, 730 F.3d 1040, 1044 (9th Cir. 2013); United States v. Deppish, 994 F. Supp. 2d 1211, 1214 (D. Kansas 2014). Rather, a warrant authorizing collection of evidence of a CFAA violation comes closer to warrants seeking to collect evidence regarding violations of broad federal statutes prohibiting fraud or conspiracy. In these cases, limitation by reference to the broad statute fails to impose any real limitation. See United States v. Maxwell, 920 F.2d 1028, 1033 (D.C. Cir. 1990) ("Although a warrant's reference to a particular statute may in certain circumstances limit the scope of the warrant sufficiently to satisfy the particularity requirement . . . it will not do so where, as here, the warrant authorizes seizure of all records and where, as here, the reference is to a broad federal statute, such as the federal wire fraud statute."); Rickert v. Sweeney, 813 F.2d 907, 909 (8th Cir. 1987) (general search limited only by broad tax evasion statute held overly broad, where probable cause existed only to search for evidence of tax evasion in connection with one particular project); United States v. Roche, 614 F.2d 6, 7-8 (1st Cir. 1980) (warrant's limitation of search to "fruits and instrumentalities of the violation" of federal mail fraud statute was inadequate because "limitation by so broad a statute is no limitation at all.").

The Google Warrant provides no other details to clarify the particular crime at issue. Section II(a) makes reference to "unauthorized network activity," yet gives no indication as to the meaning of this phrase, which would seem to be implicated in almost all of the activities prohibited by the CFAA. The warrant offers nothing about the time frame of the offense. See United States v. Hanna, 661 F.3d 271, 287 (6th Cir. 2011) (noting, in upholding search warrant for electronic information, that the warrant was limited to "the time period that the evidence suggested the activity occurred.") Rather, it provides for the seizure of all evidence of violations of the CFAA "since account inception." (Google Warrant, 6).

Although the test for particularity "is a pragmatic one," and must consider "the circumstances and type of items involved," Torch, 609 F.2d at 1090, the record does not indicate that circumstances of the investigation precluded a more particularized description of the crime. Special Agent Ahearn's supporting affidavit provides copious details as to the time and nature of the alleged offenses. Had the Google Warrant properly attached or incorporated this affidavit, it could have provided the necessary context for the search. Hurwitz, 459 F.3d at 471 ("[A]n affidavit may provide the necessary particularity for a warrant if it is *either* incorporated into *or* attached to the warrant.") (quoting United States v. Washington, 852 F.2d 803, 805 (4th Cir. 1988)). Yet the Google Warrant makes no incorporation, and it does not appear from the record that the affidavit was attached. Without the Google Warrant somehow including the additional details provided by Special Agent Ahearn's affidavit, the affidavit itself cannot satisfy concerns for particularity or overbreadth. See Groh v. Ramirez, 540 U.S. 551, 557 (2004) ("The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents.").

"[T]here are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant or search for physical objects whose relevance is more easily ascertainable." Williams, 592 F.3d at 523-24 (quoting Andresen v. Maryland, 427 U.S. 463, 482 n. 11). "Because electronic devices could contain vast quantities of intermingled information, raising the risks inherent in over-seizing data . . . law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence." Schesso, 730 F.3d at 1042; see also In the Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 166-67 (D.D.C. 2014) ("D.D.C. Mac.com Order"). Especially in light of the nature of the search and seizure here, the Google Warrant is not drafted with sufficient particularity. In the absence of additional details, the warrant fails to identify the "particular crime" for which officers were to seek evidence. Therefore, the warrant lacks the particularity required by the Fourth Amendment.

2. Good Faith

Despite the Google Warrant's lack of particularity in describing the crime at issue, the evidence seized need not be suppressed. Generally, in cases involving evidence obtained in violation of the Fourth Amendment, the exclusionary rule will preclude use of that evidence in a criminal proceeding against the victim of the illegal search and seizure. Illinois v. Krull, 480 U.S. 340, 347 (1987). However, the Supreme Court has explained that the "prime purpose" of the exclusionary rule "is to deter future unlawful police conduct." Id. In United States v. Leon, the Court explained that, "where the officer's conduct is objectively reasonable, excluding the evidence will not further the ends of the exclusionary rule in any appreciable way." United States v. Leon,

468 U.S. 897, 919-20 (1984). Consequently, Leon held that the fruits of a search conducted pursuant to a warrant, even an illegal warrant, may not be suppressed unless "a reasonably well trained police officer would have known that the search was illegal despite the magistrate's authorization." Id., at 922 n. 23. "Usually, searches conducted pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish a law enforcement officer has acted in good faith in conducting the search." Perez, 393 F.3d at 461.

Special Agent Ahearn prepared a detailed affidavit describing the illegal acts for which defendant was suspected, and presented it to a magistrate. As noted, had the warrant incorporated or attached the affidavit, it would have met Fourth Amendment concerns. Hurwitz, 459 F.3d at 471 ("[A]n affidavit may provide the necessary particularity for a warrant if it is *either* incorporated into *or* attached to the warrant."). Admittedly, there is limited caselaw within this circuit which would have alerted government agents that the statute referenced to cabin the scope of items seized pursuant to the search, the CFAA, was too broad and general to impose a meaningful limitation. It was objectively reasonable for the government to presume that the items to be seized as evidence of CFAA violations concerned the criminal activity described in the affidavit.

> The "good faith" exception does not apply in four "limited situations":
>
> > (1) when the affiant based his application on knowing or reckless falsity; (2) when the judicial officer wholly abandoned his role as a neutral and detached decision maker and served merely as a "rubber stamp" for the police; (3) when the affidavit supporting the warrant was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) when the warrant was so facially deficient that the executing officers could not reasonably have presumed that the warrant was valid.

United States v. Wellman, 663 F.3d 224, 228-29 (4th Cir. 2011).

This case does not fit any of those situations. There is no indication that the magistrate judge was misled, or "wholly abandoned" his role. Furthermore, Special Agent Ahearn's affidavit alleged that records obtained from SOLN employees indicated the shahnn28@gmail.com account was communicating with employees and investors on the dates when the alleged intrusion into the SOLN network was taking place, and that these communications discussed "security issues." (Aff. at ¶ 14) (DE 35-4). This might suggest that the account user was involved in the intrusion. It could also suggest that the account was used in preparation to commit the intrusion. Special Agent Ahearn also stated that his training and experience indicated that "evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files." (Aff. ¶ 25) (DE 35-4). The email account information that the government sought to obtain could be useful in establishing the identity of the account holder and in disclosing communications concerning an intrusion of the SOLN network. The account holder's identity was important in showing who was responsible for sending emails to SOLN employees around the dates of the attack. The email account may also have revealed other communications sent by defendant concerning the intrusion, along with information about potential conspirators. The affidavit set forth adequate allegations to "warrant a man of reasonable prudence" in believing that the items proposed to be seized would supply evidence of the crime described. Hurwitz, 459 F.3d at 473.

Nor does this case implicate Leon's exception for circumstances when the warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." Leon, 468 U.S. at 923. The warrant does reference a particular federal *statute*, even if the particular *crime* is not

detailed. As explained, there is no clear precedent within this circuit which would demonstrate to an officer that a warrant restricting seizures to evidence of CFAA violations would fail to satisfy concerns for particularity. Meanwhile, the legal standards for searching and seizing electronic evidence remains in a state of development, where courts have suggested that relaxed standards apply. See United States v. Grimmett, 439 F.3d 1263, 169 (10th Cir. 2006) ("[W]e have adopted a somewhat forgiving stance when faced with a 'particularity' challenge to a warrant authorizing the seizure of computers."); In the Matter of a Warrant for All Content and Other Info. Associated with the Email Account [redacted]@gmail.com Maintained at Premises Controlled by Google, Inc., — F. Supp. 2d —, 2014 WL 3583529, at *5 (S.D.N.Y. 2014) ("S.D.N.Y. Google Order") ("[C]ourts developed a more flexible approach to the execution of search warrants for electronic evidence."). A number of courts have authorized the government to obtain the entire contents of an email account in order to later determine which particular emails come within the scope of a search warrant. See S.D.N.Y. Google Order, — F. Supp. 2d —, 2014 WL 3583529 at *6 (citing cases). At least one other court upheld a warrant similar to the Google Warrant at issue here, that required the "disclosure" of all contents of an email, but specified the information to be seized by reference to a particular federal statute. Deppish, 994 F. Supp. 2d at 1215 (authorizing seizure of "information concerning activities and identification of any individuals related to crimes of sexual exploitation of minors pursuant to 18 U.S.C. § 2252."). The Google Warrant's deficiencies were not so patently obvious that an officer could not "reasonably have presumed" its validity. Therefore, the evidence seized pursuant to the Google Warrant will not be suppressed.

3. "Disclosure" Under Attachment B, Section I

Defendant argues that all of the information "disclosed" under Attachment B was effectively "seized" by the government, "even though most of that information had not been authorized for seizure pursuant to the warrant itself." (Mot. To Suppress Email and Related Evidence, 5). As an initial matter, the premise of defendant's argument is incorrect. As noted above, the Google Warrant referenced Attachment B for the "property to be seized." (Id., 2). Attachment B included both the information to be "disclosed," under Section I, and the information to be "seized," under Section II. (Id.) The Google Warrant thus approved the procedure set forth in Attachment B for a disclosure of information pursuant to Section I, followed by a review of the disclosed information and a "seizure" of the information noted in Section II.

This two-step procedure is acceptable under the Fourth Amendment.

> When a search requires review of a large collection of items, such as papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . . If, in those circumstances, documents not covered by the warrant are improperly seized, the government should promptly return the documents or the trial judge should suppress them.

United States v. Williams, 592 F.3d 511, 519-20 (4th Cir. 2010) (quoting Andresen, 427 U.S. at 482 n. 11). Williams recognized that a search of a computer impliedly authorized "at least a cursory review of each file on the computer." Id., at 522. Analogously, an authorized search of an email account would permit a "cursory review" of emails within the account. Documents not covered by the warrant should be suppressed. Williams, 592 F.3d at 520. Yet defendant has failed to identify any document seized which fell outside of the Google Warrant's scope.

The two-step procedure which the government employed here is expressly authorized by Federal Rule of Criminal Procedure 41(e)(2)(B). This subsection provides that "[a] warrant . . . may

authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 42(e)(2)(B). As the 2009 advisory committee's note explains,

> Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

Courts have held that two-step procedures such as this are reasonable under the Fourth Amendment in the context of obtaining electronic information from computers for off-site searches. Schesso, 730 F.3d at 1046; United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a sufficient chance of finding some needles in the computer haystack.") (quotation marks omoitted); United States v. Stabile, 633 F.3d 219, 234 (3d Cir. 2011) (rejecting on-site search requirement of hard drives because the "practical realities of computer investigations preclude on-site searches"). More recently, courts have also upheld these procedures when applied to seizures of email account information. United States v. Tsarnaev, — F. Supp. 3d —, 2014 WL 5308087, at *10-11 (D. Mass. 2014); S.D.N.Y. Google Order, — F. Supp. 2d —, 2014 WL 3583529, at *11-12; D.D.C. Mac.com Order, 13 F. Supp. 3d at 165. Following these cases, the court finds the procedure prescribed by the Google Warrant constitutional.

4. Methods to Minimize Search of Unauthorized Emails and Computer Data

Defendant also argues that the Google Warrant violated the Fourth Amendment by failing to include a procedure to "at least minimize the unreasonable intrusion into Fourth Amendment protected areas." (Mot. To Suppress Email and Related Evidence, 9). Defendant proposes that "[a]t the least, segregation should have been ordered to be executed by a filter-team consisting of agents or specially-trained computer personnel who are not involved in the investigation." (Id., 11).

Contrary to defendant's argument, "[n]othing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed." United States v. Grubbs, 547 U.S. 90, 98 (2006). A number of federal courts that have considered search warrant applications related to email accounts have refrained from requiring the government to undertake particular search methods or adopt specified document filters. See S.D.N.Y. Google Order, — F. Supp. 2d —, 2014 WL 3583529, at *11-12 ("To limit the government's computer search methodology *ex ante* would give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents or other creative data concealment techniques . . . . Our inability to predict the best mechanism for conducting a search strongly counsels against including any search protocol in a warrant.") (quoting United States v. Bowen, 689 F.Supp. 2d 675, 681 (S.D.N.Y. 2010) (quotation marks omitted); Deppish, 994 F. Supp. 2d at 1220 ("[N]othing in § 2703 precludes the Government from requesting the full content of a specified email account, nor has the Tenth Circuit ever required warrants to identify a particularized search strategy."); United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011) ("The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are

relevant before copies are obtained from the internet service provider for subsequent searching.").

While defendant has cited case law to the contrary, the reasoning of defendant's cited decisions has been questioned even within their own jurisdictions. See In the Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., No. 2014 WL 945563 (D.D.C. March 7, 2014), superseded by opinion 13 F. Supp. 2d 145, 2014 WL 1377793 (D.D.C. Apr. 7, 2014), order vacated by D.D.C. Mac.com Order, 13 F. Supp. 3d 157; In re Search Warrants for Search Warrants for Info. Assoc. With Target Email Address, No. 12-MJ-8119, 2012 WL 4383917 (D. Kan. Sept. 21, 2012), declined to follow by Deppish, 994 F. Supp. 2d at 1221.

Here the court will not require law enforcement to detail particular methods for searching documents in advance of obtaining those documents. Even requirements to delegate searching functions to filter-teams officers who are not a part of the investigation may impose an undue restraint on law enforcement efforts. Such "outsiders" to an investigation may fail to recognize particular codes, concealment techniques, or other details that would not escape the notice of an officer more familiar with the circumstances of a case.

5. Allegation that Government Search Exceeded Scope of Warrants

Defendant also alleges that the search and seizure of email content exceeded the scope of the search authorized by the warrant, and demands an evidentiary hearing to develop the argument. "[T]he manner in which a warrant is executed is subject to later judicial review as to its reasonableness." Dalia v. United States, 441 U.S. 238, 258 (1979). "When material facts that affect the resolution of a motion to suppress . . . are in conflict, the appropriate way to resolve the conflict

is by holding an evidentiary hearing after which the district court will be in a position to make findings." United States v. Taylor, 13 F.3d 786, 789 (4th Cir. 1994).

Evidentiary hearings on motions to suppress are not granted as a matter of course, but "only if the motion is sufficiently specific, non-conjectural, and detailed to enable the court to conclude that (1) the defendant has presented a colorable constitutional claim, and (2) there are disputed issues of material fact that will affect the outcome of the motion to suppress." United States v. McKoy, No. 5:09-CR-51-BO, 2011 WL 579111, at *2 (E.D.N.C. 2011) (quoting United States v. Hines, 628 F.3d 101, 105 (3rd Cir. 2010)); see also United States v. Francois, 715 F.3d 21, 32 (1st Cir. 2013) ("A hearing is required only if the movant makes a sufficient threshhold showing that material facts are in doubt or dispute, and that such facts cannot reliably be resolved on a paper record."); United States v. Curlin, 638 F.3d 562, 564 (7th Cir. 2011). The defendant bears the burden of identifying the disputed issue and demonstrating materiality. See Curlin, 638 F.3d at 564; McKoy, 2011 WL 579111, at *2.

Defendant has failed to make the necessary showing. He conclusorily alleges that "[w]here the extent of searches of [defendant's] email account is unclear, but where it appears that an unguided and unrestricted general rummaging occurred, the Court should conduct an evidentiary hearing to determine whether there were Fourth Amendment violations in the execution of the searches." (Mot. To Suppress Email and Related Evidence, 17). Defendant fails to provide any specific facts supporting that such a "general rummaging," outside the warrant's broad scope, occurred. In Tsarnaev, the court found that allegations nearly-identical to these were insufficient to reach the threshold for an evidentiary hearing on the reasonableness of a warrant's execution.

Tsarnaev, — F. Supp. 3d —, 2014 WL 5308087, at *15. The court likewise finds defendant's allegations here to be too vague and conjectural.

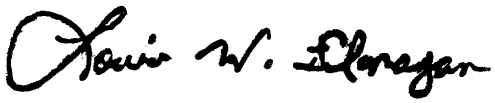
C. Motion to Suppress Evidence in Violation of Fifth Amendment Right to Counsel (DE 23)

As noted above, the government has affirmed that it will not attempt to introduce in its case in chief the statements or conduct noted in defendant's motion to suppress asserting violations of the Fifth Amendment (DE 23). Accordingly, defendant's motion is denied without prejudice, on the ground of mootness.

**CONCLUSION**

For the foregoing reasons, the court hereby DENIES defendant's motions to suppress. (DE 23, 24, 25). The clerk now will set the matter for arraignment and trial at the court's next regular criminal term no sooner than 45 days from date of entry of this order.

SO ORDERED, this the 6th day of January, 2015.



LOUISE W. FLANAGAN
United States District Judge